

Feb 12, 2021

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

11 WhatsApp accounts)

Case No. 21-M-318 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2-26-21 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Stephen C. Dries

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 2-12-21 11:00 am

Stephen C. Dries
 Judge's signature

City and state: Milwaukee, Wisconsin

Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <div style="text-align: right; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: right;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following phone numbers and for the following periods, that are stored at premises controlled by WhatsApp, a company that accepts service of legal process at 1601 Willow Road in Menlo Park, California.

1. **(202) 921-0123** (from January 1, 2016 to present)
2. **(202) 753-9708** (from January 1, 2016 to present)
3. **+91-7054210000** (from January 1, 2016 to present)
4. **+91-8765919198** (from January 1, 2016 to present)
5. **+91-9044971271** (from January 1, 2016 to present)
6. **+54-911 36594384** (from January 1, 2016 to present)
7. **+90-5368406561** (from January 1, 2016 to present)
8. **+91-7304096699** (from June 1, 2018 to present)
9. **+91-9356460394** (from June 1, 2018 to present)
10. **+34-691962857** (from June 1, 2018 to present)
11. **+44-7490620584** (from August 1, 2019 to present)

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by WhatsApp (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each of the accounts or identifiers listed in Attachment A:

- a. All stored electronic communications (including drafts, sent items, deleted items, stored backup copies, and attachments) and other stored content information contained in or on behalf of the accounts.
- b. All histories, profiles, contact lists, email addresses, attachments, screen names, name, age, telephone number, physical address, or user IDs, associated with the accounts;
- c. Logs of all access to the accounts, including but not limited to all electronic communications sent to or from the account, including dates, times of access, and the Internet Protocol addresses (IP addresses) from which the account was accessed, for the accounts;
- d. All transactional information concerning activity associated with the accounts, including log files, dates, times, methods of connecting, or locations, for the accounts;
- e. All business records and subscriber information, in any form kept, concerning the accounts, including applications, account creation date and time, all full names, screen names, and account names associated with the subscribers, profile photos, contact lists, group chats, methods of payment, telephone numbers, addresses, and detailed billing records, for the accounts; and
- f. All records indicating the services available to subscribers of the account.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 841(a)(1), 841(h), and 843(c)(2)(A), including but not limited to:

- a. The sale and distribution of controlled substances;
- b. The exchange or laundering of funds related to the sale and distribution of controlled substances;
- c. Evidence indicating how and when the WhatsApp account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the WhatsApp account owner;
- d. Evidence indicating the WhatsApp account owner's state of mind as it relates to the crimes under investigation;
- e. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s)
- f. Other accounts used by the persons using the account;
- g. The devices used to access the account;
- h. The identity of the person(s) who communicated with the account about matters relating to the sale and distribution of controlled substances, including records that help reveal their whereabouts;
- i. Financial information, credit card numbers, social security numbers, and other personal identifiable information stored on/in the WhatsApp account; and
- j. Communications and files that contain IP addresses and username and passwords.

Feb 12, 2021

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

11 WhatsApp accounts

Case No.

21-M-318 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 846, 841(a)(1), 841 (h), and 843(c)(2)(A)	distribution of a controlled substance, possession with intent to distribute a controlled substance, internet distribution of controlled substances, and conspiracy to do the same

The application is based on these facts:

See the attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SCOTT SIMONS (Affiliate) Digitally signed by SCOTT SIMONS (Affiliate)
Date: 2021.02.12 10:08:28 -06'00'

Applicant's signature

Scott Simons, Task Force Officer (DEA)

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 02/12/2021

Stephen C. Dries

Judge's signature

City and state: Milwaukee, Wisconsin

Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Scott Simons, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a WhatsApp account that is stored at premises owned, maintained, controlled, or operated by WhatsApp LLC, a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require WhatsApp to disclose to the government records and other information in its possession, pertaining to the subscribers or customers associated with the specified WhatsApp accounts.

2. I am a Task Force Officer assigned to the Milwaukee District Office of the Drug Enforcement Administration (DEA) as a member of the Tactical Diversion Squad (TDS). I specialize in pharmaceutical investigations. I have worked full-time as a federal task force officer for the past 7 years and a full-time law enforcement officer with the Greenfield Police Department for the past 18 years. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

3. During my tenure as a law enforcement officer, I have been involved in the investigation of drug traffickers in Milwaukee County, in the State of Wisconsin, across the United States, and internationally. I have received training in the investigation of drug trafficking, money laundering, and computer crimes. I have worked with informants in the investigations of drug trafficking. I have participated in the application for and execution of

numerous search warrants. I have participated directly in numerous narcotics investigations and arrests in which controlled substances and drug paraphernalia were seized. I am familiar with methods that are commonly used by drug traffickers to package and prepare controlled substances for sale.

4. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, publicly available information, and from persons with knowledge of relevant facts. Because this affidavit is submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

5. Based on the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the accounts identified in Attachment A, will contain evidence and instrumentalities related to violations of Title 21, United States Code, Sections 846 (conspiracy to distribute and possess with the intent to distribute a controlled substance), 841(a)(1) (distribution of a controlled substance), 841(h) (distribution of a controlled substance by means of the Internet), and 843(c)(2)(A) (use of the Internet to advertise or offer the sale of a controlled substance), as further described in Attachment B.

STATUTORY BACKGROUND

6. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 amended the Controlled Substances Act to address online pharmacies, codified at Title 21, United States Code, Section 829. No controlled substance that is a prescription drug as determined by the Federal Food, Drug and Cosmetic Act may be delivered, distributed, or dispensed by means of the Internet without a valid prescription, as required by Title 21, Code of Federal Regulations,

Section 1306.09(a).

7. According to Section 829, the term “valid prescription” means a prescription that is issued for a legitimate medical purpose in the usual course of professional practice by a practitioner who has conducted at least 1 in-person medical evaluation of the patient or a covering practitioner. The term “in-person medical evaluation” means a medical evaluation that is conducted with the patient in the physical presence of the practitioner, without regard to whether portions of the evaluation are conducted by other health professionals. The term “covering practitioner” means, with respect to the patient, a practitioner who conducts a medical evaluation (other than an in-person medical evaluation) at the request of a practitioner who has conducted at least 1 in-person medical evaluation of the patient or an evaluation of the patient through the practice of telemedicine within the previous 24 months and is temporarily unavailable to conduct the evaluation of the patient.

8. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 also added new provisions to prevent the illegal distribution of controlled substances by means of the Internet, including registration requirements of online pharmacies, Internet pharmacy website disclosure information requirements, and prescription reporting requirements for online pharmacies.

PROBABLE CAUSE

9. In 2015, the Milwaukee District Office of the DEA initiated an investigation into the internet pharmacy GOLDPHARMA24 located at www.goldpharma-24.com, which advertised controlled and non-controlled pharmaceuticals for sale without requiring a prescription. During the course of the investigation of GOLDPHARMA24, case agents identified a co-conspirator in Florida (hereinafter referred to as “SOI-1”) and a co-conspirator in Texas

(hereinafter referred to as “SOI-2”). These two co-conspirators were working together to receive bulk shipments of controlled pharmaceuticals and reship them to customers throughout the United States. Case agents interviewed these two co-conspirators and executed federal search warrants at their residences. These co-conspirators identified multiple drug suppliers, Google email accounts, and WhatsApp accounts used by their drug suppliers to conduct drug transactions.

10. Case agents began this investigation into the drug suppliers using PILL2DAYS, BUYETIZOLAM, and PREMIER MEDICAL AGENCY based on evidence acquired from the cooperating co-conspirators. Case agents conducted multiple controlled buys and communicated with the drug suppliers, including by the Google email accounts and WhatsApp accounts belonging to those drug suppliers. According to DEA records, PILL2DAYS, BUYETIZOLAM, and PREMIER MEDICAL AGENCY are not registered online pharmacies. As described below, probable cause exists to believe that the Google email accounts and WhatsApp accounts associated with the phone numbers identified in Attachment A were used to facilitate the offenses described above.

11. An undercover agent in the Eastern District of Wisconsin purchased controlled pharmaceuticals numerous times from SOI-1 and SOI-2 between July 2019 and August 2020. The primary method of communication between the undercover agent and SOI-1 was via WhatsApp. Subsequent analysis of these suspected controlled substances by the DEA laboratory, identified controlled substances including heroin, methamphetamine, ketamine, tramadol, diazepam, alprazolam, and modafinil.

12. In August 2020, case agents executed federal search warrants in Florida and Texas at the residences of SOI-1 and SOI-2. Case agents seized electronic devices and

documents containing evidence identifying many of the drug suppliers and customers, communication related to the sale of controlled substances, and money laundering of drug proceeds. Case agents also seized approximately \$100,000 in drug proceeds and different types of suspected controlled pharmaceuticals. Case agents have had the opportunity to interview SOI-1 and SOI-2 multiple times about the various drug suppliers and the circumstances around communication with the suppliers and drug payments to the suppliers.

13. SOI-1 said that he began as a payment processor. In June 2018, SOI-1 was contacted online by the co-owners of the online pharmacies www.buyetizolam.com (“BUYETIZOLAM”) and www.compratapentadol.com (“COMPRATAPENTADOL”). According to SOI-1, BUYETIZOLAM sells etizolam (an unapproved drug in the United States) and modafinil (a Schedule IV controlled substance), and COMPRATAPENTADOL sells tapentadol (a Schedule II controlled substance), modafinil (a Schedule IV controlled substance), tramadol (a Schedule IV controlled substance), and carisoprodol (a Schedule IV controlled substance). SOI-1 said that at least 98% of their sales are to customers in the United States. SOI-1 processed payments for all the orders placed on these websites, and SOI-1 provided case agents with a list of all these orders, which included the identity of the customer, address of the customer, and amount paid for the drugs. SOI-1 identified the primary drug supplier for these websites as AKSHAY SAKODE, who is the owner of India-based distributor, PREMIER MEDICAL AGENCY. SOI-1 was directed to forward half of the processed drug payments to the owners of these websites and the other half to AKSHAY SAKODE. In total, SOI-1 transferred in excess of \$1,000,000 in U.S. currency in drug proceeds to bank accounts belonging to AKSHAY SAKODE and bank accounts belonging to the owners of the websites.

14. SOI-1 stated there are three co-owners of BUYETIZOLAM and

COMPRATAPENTADOL. SOI-1 told the owners that he would not do business with them unless they were open with him about the operation. SOI-1 identified the owners as the following:

- DAVID PIERRE LETTINGA – 40% owner
- KEVIN VAN DER HULST – 40% owner
- Ben – 20% owner

15. SOI-1 primarily communicated with LETTINGA, who is an equal owner with VAN DER HULST. SOI-1 communicated with LETTINGA, via WhatsApp at phone number **+34-691962857**, and email address **tinuschicken@gmail.com**. SOI-1 sent the majority of the drug proceeds to LETTINGA's personal bank account in Germany. LETTINGA is a citizen of the Netherlands, but resides in Spain. SOI-1 maintained an Excel spreadsheet file of all drug payments that SOI-1 processed for BUYETIZOLAM and COMPRATAPENTADOL, and saved this Excel file in Google Drive. LETTINGA had access to this file by using the email account **tinuschicken@gmail.com**. In addition, SOI-1 communicated with LETTINGA about drug orders, drug proceeds, and other drug business at email address **tinuschicken@gmail.com** and WhatsApp phone number **+34-691962857**.

16. SOI-1 reported that VAN DER HULST was primarily in charge of the technical side of the drug conspiracy by creating and maintaining the online pharmacy websites. SOI-1 communicated with VAN DER HULST by telephone and email several times and also sent drug proceeds to VAN DER HULST's personal bank account in the Netherlands, where VAN DER HULST resides.

17. The third owner of BUYETIZOLAM and COMPRATAPENTADOL is only known by SOI-1 as "Ben." Ben taught LETTINGA and VAN DER HULST how to run an illegal

online pharmacy business. Ben is a 20% owner, owns additional online pharmacies, and is not engaged in the day-to-day operations with BUYETIZOLAM and COMPRATAPENTADOL. SOI-1 believes Ben resides in Holland.

18. BUYETIZOLAM and COMPRATAPENTADOL websites are supplied by Indian pharmaceutical distributor PREMIER MEDICAL AGENCY, which is owned by AKSHAY SAKODE. SOI-1 would transfer half of the drug proceeds to LETTINGA and VAN DER HULST and the other half to SAKODE's bank account in India. SOI-1 also utilized PREMIER MEDICAL AGENCY as SOI-1's drug supplier for regular bulk drug shipments to SOI-1's partner SOI-2 in Texas. These drug shipments were broken down and reshipped to U.S. customers. SOI-1 stated some of these drugs were shipped to undercover case agents in the Eastern District of Wisconsin. SOI-1 communicated with SAKODE, via WhatsApp at phone number **+91-7304096699**, and Google email address **pmagency**sales@gmail.com****. The communication with SAKODE via WhatsApp and email, consisted of communication related to drug orders and drug payments.

19. SOI-1 identified another online pharmacy www.pill2days.com ("PILL2DAYS"), from which SOI-1 had purchased Xanax (a Schedule IV controlled substance) and suspected Adderall (a Schedule II controlled substance) in the summer of 2020. SOI-1 communicated with the website representative via email at email address **r.stewarts121514@gmail.com**. Case agents later reviewed these emails and saw the discussion of controlled substances being shipped from overseas to the United States, domestically from re-shippers located in the United States, prices, a drug photograph, and quantities. SOI-2 was responsible for sending the drug payment, so SOI-2 communicated with a website representative via telephone at a phone number known to be used by the online pharmacy PILL2DAYS.

20. SOI-1 and SOI-2 were told by PILL2DAYS representatives that they ship pharmaceuticals from overseas to U.S. customers at the advertised prices on the website. At a significantly higher price, U.S. customers can receive the drug parcels from domestic re-shippers they have established. SOI-1 stated he was aware of re-shippers in Arizona and Florida. Case agents were able to intercept and seize a parcel from PILL2DAYS to SOI-2, which was supposed to contain 360 tablets of Adderall. This parcel was shipped by a re-shipper in Vermont. These tablets were sent to the DEA laboratory, and found to contain 364 tablets of modafinil (a Schedule IV controlled substance).

21. Case agents reviewed the PILL2DAYS online pharmacy website www.pill2days.com. This website offers the following controlled substances for sale:

- Adderall – a Schedule II controlled substance
- Phentermine – a Schedule IV controlled substance
- Diazepam – a Schedule IV controlled substance
- Ativan – a Schedule IV controlled substance
- Klonopin – a Schedule IV controlled substance
- Xanax – a Schedule IV controlled substance
- Ambien – a Schedule IV controlled substance
- Soma (carisoprodol) – a Schedule IV controlled substance
- Tramadol - a Schedule IV controlled substance.

22. SOI-1 and SOI-2 both identified a “broker” located in the United Kingdom, who was known as DAVE ADDISON JR. ADDISON communicated about drug orders, drug payments, and drug shipments, only via a WhatsApp account linked to phone number **+44-7490620584**. SOI-2 was the only one who communicated with ADDISON, but the drugs

received from ADDISON were supplied to the customers belonging to both SOI-1 and SOI-2. Multiple types of controlled pharmaceuticals were purchased from ADDISON, received by SOI-2, and then reshipped to customers in the United States. SOI-1 and SOI-2 stated that the Adderall 30mg, which later tested positive for methamphetamine, and Percocet 10mg, which tested positive for methamphetamine, heroin, tramadol, and caffeine, which SOI-1 and SOI-2 shipped to undercover case agents during controlled purchases were supplied by ADDISON. All of these purchases from ADDISON were conducted by communicating via the WhatsApp account linked to phone number **+44-7490620584**. All drug payments were made via Bitcoin to different Bitcoin addresses provided by ADDISON via WhatsApp.

23. SOI-1 and SOI-2 stated that ADDISON was just the broker taking the drug orders on behalf of a shipper located in the United Arab Emirates (UAE). Based on financial and shipping records reviewed by case agents, the drug parcels appear to be originating from Pakistan and then shipped through the UAE to the United States. SOI-1 and SOI-2 provided the identity of several other U.S. customers receiving drug shipments from ADDISON. SOI-1 and SOI-2 stated that once a drug parcel arrived and the drugs were damaged. SOI-2 told ADDISON that SOI-2 was going to return the drug parcel to ADDISON. ADDISON provided an address in London, United Kingdom and directed SOI-2 to ship the drugs to that location. SOI-2 and SOI-1 believe for this reason, and because ADDISON's phone number has a United Kingdom country code, that ADDISON is located in the United Kingdom. Case agents reviewed emails and SOI-2's cell phone and were able to confirm these details regarding ADDISON, including ADDISON's phone number **+44-7490620584**.

24. SOI-1 and SOI-2 provided additional details related to the aforementioned drug suppliers, as well as other suppliers, and case agents were able to corroborate the information as true and accurate.

25. On November 24, 2020, case agents began communicating with ADDISON via WhatsApp at phone number **+44-7490620584**. ADDISON messaged case agents a list of approximately 23 different medications for sale, including Percocet 10mg and Adderall 30mg. These are the same medications SOI-1 and SOI-2 purchased from ADDISON and reshipped to undercover agents. Case agents and ADDISON discussed shipping, drug quantities, and pricing. ADDISON stated that Bitcoin was the only accepted form of payment and provided additional details, which matched the information provided by SOI-1 and SOI-2. Case agents informed ADDISON that case agents operated a domestic reshipping operation in the United States. ADDISON solicited case agents to receive bulk parcels from ADDISON and reship the drugs to ADDISON's customers. Case agents informed ADDISON that this was a possibility in the future, but first case agents wished to become an established customer. This entire communication was conducted via the WhatsApp account linked to phone number **+44-7490620584**.

26. On December 1, 2020, case agents conducted an undercover purchase from BUYETIZOLAM via the website. Case agents purchased 500 tablets containing a mixture of tapentadol 150mg (a Schedule II controlled substance) and etizolam 2mg (an unapproved drug in the United States). In connection with the purchase, case agents were directed via email to conduct a bank transfer to an account with TransferWise. Case agents received the shipment of the 500 tablets of the tapentadol and etizolam mixture in blister packs, which were shipped from

India by the shipper PREMIER MEDICAL AGENCY. The medications were sent to the DEA laboratory in Chicago, and the test results are pending.

27. Case agents later received records from TransferWise, pursuant to a DEA administrative subpoena, related to the customer account to which undercover agents sent the drug payment. This TransferWise account belongs to DAVID PIERRE LETTINGA in Spain. Records revealed that funds from this account were also transferred to another account listing to KEVIN VAN DER HULST.

28. On December 1, 2020, case agents conducted an undercover purchase from PILL2DAYS via the telephone number (202) 753-9072, which is published on the website. Case agents purchased 180 tablets of Adderall 30mg (a Schedule II controlled substance). In connection with the purchase, case agents were directed via text message to conduct a bank transfer by Zelle to a bank account linked to the phone number (828) 215-5158 and the first name "Jawed." Case agents received the shipment of the 180 tablets of suspected Adderall 30mg, which was shipped from Vermont. The substances were sent to the DEA laboratory in Chicago, and the analysis revealed the presence of tramadol (a Schedule IV controlled substance).

29. Case agents later received records from T-Mobile, pursuant to a DEA administrative subpoena, requesting records related to phone number (828) 215-5158. The records revealed that the account is registered to a specific address in Apex, North Carolina. Case agents accessed files available to the DEA and fully identified a resident at this address with the first name "Jawed" (hereinafter referred to as "SOI-3"). Case agents later confirmed SOI-3 is the person who received the drug payment.

30. On December 11, 2020, case agents conducted an undercover purchase from PILL2DAYS, via the telephone number (202) 753-9072, which is published on the website. Case agents purchased 180 tablets of hydrocodone 10mg (a Schedule II controlled substance). In connection with the purchase, case agents were directed via text message to conduct a bank transfer by Zelle, to a bank account linked to the email address info@vigordose.com and name “Annie Abraham.” Case agents were sent the tracking number by text message and by email from r.stewarts121514@gmail.com. This email contained an email signature “Robbie Stewart – Sales Manager.” Case agents received the shipment of the 180 tablets of suspected hydrocodone 10mg which was shipped from Green Bay, Wisconsin. The medication was sent to the DEA laboratory in Chicago, and the analysis revealed the presence of tramadol (a Schedule IV controlled substance).

31. Case agents have identified “Annie Abraham” as ANNAMMA ABRAHAM, who is a suspected payment processor in New York. Case agents identified that the drug shipper located in Green Bay, Wisconsin also shipped an additional five parcels at the same time as the drug parcel received by case agents.

32. On December 21, 2020, case agents conducted an undercover purchase directly from WhatsApp via Indian telephone number +91-7304096699. SOI-1 had identified this phone number as belonging to AKSHAY SAKODE, the owner of PREMIER MEDICAL AGENCY. Case agents purchased 2,000 tablets of tapentadol 100mg (a Schedule II controlled substance) and 1,000 tablets of modafinil (a Schedule IV controlled substance). In connection with the purchase, case agents were directed via WhatsApp message from +91-7304096699 and email pmagency-sales@gmail.com, to conduct a bank transfer to bank account PREMIER MEDICAL AGENCY in India. Case agents were emailed five tracking numbers from

pmagency-sales@gmail.com and further communicated with this email address about payment and the drug transaction. Many of these emails contained an email signature “AKSHAY SAKODE.” Case agents have received one of the five parcels as of this time and are monitoring the tracking of the other parcels which are still in transit from India and Singapore. The received parcel contained blister packs of approximately 600 tablets of tapentadol 100mg (a Schedule II controlled substance). The medication was sent to the DEA laboratory in Chicago, and the analysis results are pending. Case agents have further communicated with AKSHAY SAKODE about the status of the remaining drug parcels via WhatsApp phone number +91-7304096699.

33. On January 11, 2021, case agents conducted an undercover purchase from PILL2DAYS via the telephone number (202) 753-9072, which is published on the website. Case agents purchased 90 tablets of hydrocodone 10mg (a Schedule II controlled substance), 90 tablets of Xanax 2mg (a Schedule IV controlled substance), and 180 tablets of tapentadol 100mg (a Schedule II controlled substance). In connection with the purchase, case agents initially asked to make payment via Bitcoin as a ruse to identify another method of accepted payment. Case agents were provided with a Bitcoin address via text message. Case agents then requested to change the payment method to Zelle. Case agents were directed, via text message, to conduct a bank transfer by Zelle to a bank account linked to the email address info@vigordose.com and name “Annie Abraham.” Case agents were sent the tracking numbers by text message and by email from r.stewarts121514@gmail.com. This email contained an email signature “Robbie Stewart – Sales Manager.” Case agents received the shipment of the 90 tablets of suspected hydrocodone 10mg which was shipped from Green Bay, Wisconsin, the shipment of the 90 tablets of suspected Xanax 2mg which was shipped from Salem, Oregon, and the shipment of the

180 tablets of tapentadol 100mg from the Bronx, New York. The medications were sent to the DEA laboratory in Chicago, and the analysis results are pending.

34. Case agents received records from Coinbase, a cryptocurrency platform, pursuant to a DEA administrative Subpoena, related to the Bitcoin address provided to case agents for the sending of the drug payment. These records identify the account holder as KATHERINE MAHANEY residing in Oakland, California and having phone numbers (510) 508-0345 and (202) 753-9072. The phone number (510) 508-0345 is the phone number linked to a bank account that SOI-2 sent drug payment to for a drug parcel in August 2020. The phone number (202) 753-9072 is the phone number published on the PILL2DAYS website and the same phone number case agents communicate with to place controlled purchases. Furthermore, case agents have identified additional financial accounts listing to KATHERINE MAHANEY which are receiving suspected drug payments. As a result, KATHERINE MAHANEY has been identified as a suspected payment processor. As of January 7, 2021, this Coinbase account held 0.42791853 Bitcoin valued at approximately \$15,924.18 in U.S. dollars.

35. Case agents have extensively communicated with a PILL2DAYS representative who identified himself as “Michael,” via text message at phone number (202) 753-9072. “Michael” has explained that he works in a call center in India, and the prices on the PILL2DAYS website are for drug parcels shipped from India. For an additional cost, the drug parcels can be shipped from one of the many domestic re-shippers that PILL2DAYS has established throughout the United States.

36. Case agents received records from J2Web Services, Inc., a VOIP telephone services, pursuant to a DEA administrative Subpoena, related to the phone number (202) 753-9072. These records identified the following account details:

- Created Date: June 3, 2020
- Name: Robbie Stewart
- Company Name: RX202
- Email address: r.stewart01@protonmail.com
- Creation IP address: 68.123.12.232 (linked to KATHERINE MAHANEY in Oakland, CA)
- Previous email: katmahaney@hotmail.com
- Forwarding number: (510) 508-0345 (linked to KATHERINE MAHANEY)
- Billing name: KATHERINE E. MAHANEY
- Billing address: 1039 Elbert St., Oakland, CA 94602 (residence of KATHERINE MAHANEY)

37. Case agents also received text message content and voicemails from J2Web Services, Inc. Thousands of text messages and voicemails revealed numerous pharmaceutical drug transactions between the user of this telephone account and customers in the United States. Several payment methods, financial accounts, and co-conspirators were identified based on the content. It was observed that KATHERINE MAHANEY communicates regularly with the user of this telephone number (202) 753-907, she plays a financial role within the organization, and based on records is believed to be the person who created this telephone account. Case agents also observed a reference in a text message of “ASHUTOSH VAISH” in Lucknow, India.

38. Case agents learned that the Federal Bureau of Investigation in Raleigh, North Carolina was investigating “SOI-3” for processing fraud payments. Case agents spoke with FBI Special Agent Harrison Putman, who said that the FBI had executed a search warrant on the

personal residence of SOI-3 on December 3, 2020. Special Agent Putman reported that SOI-3 wished to speak with case agents about the PILL2DAYS's drug trafficking organization.

39. On January 27, 2021, case agents met with SOI-3.

40. SOI-3 stated that in approximately 2015 or 2016, he began working as a payment processor for the PILL2DAYS drug conspiracy, accepting payments in the form of credit and debit cards, wire transfers such as Zelle, electronic checks, physical checks, PayPal, and Venmo. SOI-3 was initially informed by the leader of the drug conspiracy, ASHUTOSH VAISH, that the sales were for herbal substances. SOI-3 learned from customers in 2018 that the sales were for the following controlled substances:

- Ambien (a Schedule IV controlled substance)
- Valium (a Schedule IV controlled substance)
- Xanax (a Schedule IV controlled substance)
- Klonopin (a Schedule IV controlled substance)
- Tramadol (a Schedule IV controlled substance)
- Soma (a Schedule IV controlled substance)
- Adderall (a Schedule II controlled substance)
- Oxycodone (a Schedule II controlled substance)
- Hydrocodone (a Schedule II controlled substance)

41. SOI-3 stated that ASHUTOSH VAISH is in charge of a call center in Lucknow, India, which handles all the orders, coordinates the Indian and domestic drug shippers, and coordinates the payment processors. SOI-3 has met ASHUTOSH VAISH in person in India in 2017 and 2018. Case agents showed SOI-3 known photographs of ASHUTOSH VAISH, and SOI-3 positively identified ASHUTOSH VAISH. In 2018, SOI-3 confronted ASHUTOSH

VAISH about the types of drugs being sold, and ASHUTOSH VAISH admitted the drugs were all “hard drugs” and not herbal substances because “hard drugs” are more profitable. ASHUTOSH VAISH explained to SOI-3 that ASHUTOSH VAISH has Indian shippers, but for a higher price for the customer, the drugs can be shipped from numerous re-shippers in the United States. SOI-3 identified the person who makes the websites for ASHUTOSH VAISH, as NICOLAS BIGNONE, an Argentine national who lives in Argentina. SOI-3 was introduced to NICOLAS BIGNONE and communicates with him regularly. NICOLAS BIGNONE has told SOI-3 that NICOLAS BIGNONE creates the online pharmacy websites for ASHUTOSH VAISH and others. NICOLAS BIGNONE monitors the customer sales and is paid between \$4,000 to \$5,000 up front for every 100 sales. NICOLAS BIGNONE has had SOI-3 register a business in the U.S. in order for NICOLAS BIGNONE to open bank accounts in Miami, Florida which are used to receive the payments for creating the online pharmacy websites. SOI-3 primarily transfers drug payments directly to ASHUTOSH VAISH’s bank account in India, but occasionally is instructed to transfer the funds to NICOLAS BIGNONE or other co-conspirators. SOI-3 received on average \$20,000 to \$25,000 in drug payments per month. SOI-3 said there are other payment processors throughout the United States, and SOI-3 was told by ASHUTOSH VAISH that ASHUTOSH VAISH receives \$60,000 to \$70,000 in drug payments per month. SOI-3 said that all customer payments he received were from customers in the United States.

42. SOI-3 was told by ASHUTOSH VAISH that ASHUTOSH VAISH uses the alias “Robbie Stewart.” SOI-3 communicates with ASHUTOSH VAISH via WhatsApp, email, and phone numbers listed below:

- **(202) 921-0123**
- **(202) 753-9708**

- **+91-7054210000**
- **+91-8765919198**
- **+91-9044971271**
- **robbiestewarts1909@gmail.com**
- **stewartsrobbie@gmail.com**
- **r.stewarts121514@gmail.com**
- **contact.r.stewarts@protonmail.com**
- **r.stewarts@protonmail.ch**

SOI-3 stated that communication at all of these email addresses and phone numbers included conversations about the drug conspiracy, specifically drug orders, processing payments, and movement of drug proceeds.

43. SOI-3 communicates with NICOLAS BIGNONE via WhatsApp and email listed below:

- **+54-911 36594384**
- **+90-5368406561**
- **nick23904@gmail.com**

SOI-3 stated communication at the email address and phone numbers via WhatsApp, included conversations about the drug conspiracy, creation of the websites, payments for drug purchases, creation of a business for opening domestic bank accounts, and movement of drug proceeds. SOI-3 stated that NICOLAS BIGNONE also emailed SOI-3 an image of his passport and a utility bill to assist with creating the business. NICOLAS BIGNONE messages SOI-3 personal photographs of himself traveling to various countries. SOI-3 provided case agents with these documents and some photographs of NICOLAS BIGNONE which were sent to SOI-3 via both

WhatsApp phone numbers.

44. On January 16, 2021, case agents communicated with ADDISON via WhatsApp at phone number **+44-7490620584** to conduct a controlled purchase of 500 tablets of Adderall 30mg (suspected to contain methamphetamine) and 500 tablets of Percocet 10mg (suspected to contain methamphetamine, heroin, tramadol, and caffeine). Case agents and ADDISON discussed pricing and quantity, and ADDISON said the minimum shipment that the shipper will ship is 1,000 tablets. ADDISON provided case agents with a Bitcoin address where payment should be sent. Case agents did send Bitcoins worth approximately \$3,100 to the target Bitcoin address, and ADDISON confirmed that the payment was received. Case agents have discussed this drug purchase further with ADDISON, and the drug parcel has not been received yet. The entire conversation with ADDISON was conducted by communicating via WhatsApp account linked to phone number **+44-7490620584**.

45. On January 16, 2021, case agents communicated with PREMIER MEDICAL AGENCY and AKSHAY SAKODE via email at pmagencysales@gmail.com and via WhatsApp phone number **+91-7304096699**. Case agents inquired about the availability of specific controlled substances and received a message back from WhatsApp phone number **+91-7304096699** and email address pmagencysales@gmail.com. The email included an email signature and contact information for further discussion. The email signature listed two domains for the two PREMIER MEDICAL AGENCY online pharmacy websites. Furthermore, the email signature provided phone number **+91-9356460394** to be contacted directly via phone or by Telegram, WhatsApp, or Signal regarding PREMIER MEDICAL AGENCY. Case agents reviewed the two online pharmacy websites, and one of the websites has the phone number **+91-9356460394** to be contacted for business with PREMIER MEDICAL AGENCY.

46. BUYETIZOLAM's WhatsApp records associated with phone number **+34-691962857** are being requested from June 1, 2018 to the present, because SOI-1 and records indicate that evidence should exist during this time period.

47. PREMIER MEDICAL AGENCY's WhatsApp records associated with phone numbers **+91-7304096699 and +91-9356460394** are being requested from June 1, 2018 to the present, because SOI-1 and records indicate that evidence should exist during this time period.

48. PILL2DAYS's WhatsApp records associated with phone numbers **(202) 921-0123, (202) 753-9708, +91-7054210000, +91-8765919198, +91-9044971271, +54-91136594384, and +90-5368406561** are being requested from January 1, 2016 to the present, because SOI-3 and records indicate that evidence should exist during this time period.

49. ADDISON's WhatsApp records associated with phone number **+44-7490620584** are being requested from August 1, 2019 to the present, because SOI-1, SOI-2, and records indicate that evidence should exist during this time period.

50. Case agents believe that SOI-1 is a reliable witness as SOI-1 has provided a statement against SOI-1's own penal interest, and information provided by SOI-1 has been independently corroborated by case agents. SOI-1's criminal history consists of misdemeanor assault and misdemeanor menacing. SOI-1 has no prior felony convictions. SOI-1 has provided information in other investigations, and that information was found to be accurate and reliable. SOI-1 is cooperating with law enforcement for potential consideration for his federal felony drug distribution arrest, which remains pending.

51. Case agents believe that SOI-2 is a reliable witness as SOI-2 has provided a statement against SOI-2's own penal interest, and information provided by SOI-2 has been independently corroborated by case agents. SOI-2's criminal history consists of one prior federal

felony conviction for conspiracy to commit health care fraud, mail and wire fraud, money laundering, and illegal monetary transaction, conspiracy to distribute controlled substances, and mail fraud. SOI-2 may have been arrested for forgery in the 1980s. SOI-2 has provided information in other investigations, and that information was found to be accurate and reliable. SOI-2 is cooperating with law enforcement for potential consideration in his new federal felony drug conspiracy and drug distribution case, and any revocation sentence for his supervised release in the prior case.

52. Case agents believe that SOI-3 is a reliable witness as SOI-3 has provided a statement against SOI-3's own penal interest, and information provided by SOI-3 has been independently corroborated by case agents. SOI-3's criminal history consists of one federal arrest from this investigation. SOI-3 has no prior felony convictions. SOI-3 has provided information in other investigations, and that information was found to be accurate and reliable. SOI-3 is cooperating with law enforcement for potential consideration for his federal felony fraud arrest from this investigation, which remains pending.

53. Based on my training and experience and the facts described herein, I believe BUYETIZOLAM, PREMIER MEDICAL AGENCY, PILL2DAYS, and DAVE ADDISON JR. are trafficking drugs by shipping controlled pharmaceuticals from overseas to the United States. The drugs are either shipped directly to the customers or re-shipped to customers by drug re-shippers in the United States. Co-conspirators in the United States are also operating as payment processors to facilitate the drug payments. Based on my training and experience and the facts set forth above, I believe that information related to the WhatsApp accounts linked to phone numbers: (202) 921-0123, (202) 753-9708, +91-7054210000, +91-8765919198, +91-

9044971271, +54-911 36594384, +90-5368406561, +91-7304096699, +91-9356460394, +44-7490620584, and +34-691962857 will contain evidence of these crimes.

54. I know from my training and experience that even though WhatsApp does not regularly maintain completed message content, WhatsApp records will often times provide details that enable law enforcement to identify the user of the WhatsApp account(s) and identify his or her location. In this case, the identification of the user of the WhatsApp account will assist case agents in identifying the true identity and location of the person(s) having control over the WhatsApp accounts, identification of co-conspirators, financial accounts, the identification of drug suppliers and shippers, and the identification of customers.

55. I also know that persons involved with owning or operating internet pharmacies and providing the drugs for such internet pharmacies often times communicate by WhatsApp, which is consistent with the evidence in this investigation. These communications include but are not limited to drug orders, drug shipping information, and payments for said drugs. In this investigation, I have had the opportunity to interview multiple co-conspirators who have used WhatsApp to communicate with other identified and unidentified co-conspirators. Furthermore, case agents have communicated with co-conspirators using WhatsApp. Based on the interviews of cooperating co-conspirators and undercover communication with co-conspirators, I know that WhatsApp is a primary form of communication for this drug conspiracy as it is a universal communication platform that can be utilized across many countries. WhatsApp is being used by customers to place drug orders, coordinate drug shipments, and coordinate drug payments.

56. For all of the foregoing reasons, case agents are requesting a search warrant for records and information from WhatsApp for the accounts set forth in Attachment A for the following: **(202) 921-0123, (202) 753-9708, +91-7054210000, +91-8765919198, +91-**

9044971271, +54-911 36594384, and +90-5368406561 for the period of January 1, 2016 to the present, +91-7304096699, +91-9356460394, and +34-691962857 for the period of June 1, 2018 to the present, and +44-7490620584 for the period of August 1, 2019 to the present. These beginning dates are the dates case agents are aware these internet pharmacies were in operation.

BACKGROUND REGARDING WHATSAPP MESSENGER

57. Based on my training and experience, I have learned the following about WhatsApp Messenger:

- a. WhatsApp provides an electronic communications and networking service which is available for Internet enabled “smartphones,” cellular telephones with Internet connection capabilities. Subscribers obtain an account by registering with WhatsApp after downloading and installing the “WhatsApp” application to their “smartphone” and then registering their account. WhatsApp requests subscribers to provide basic information, such as their name and telephone number. However, the only information that is verified by WhatsApp is the telephone number associated with the account;
- b. When messages and content are sent and received through the WhatsApp application, the number appears as it would if using Short Message Service (SMS) messages, commonly referred to as “text messages,” through the wireless network. However, the Internet, and not a telephone network, is the vehicle that delivers the content;
- c. The WhatsApp application allows users, through their mobile telephone service provider’s data network (i.e. the network enabling email and Internet browsing) or through a wireless network access point (i.e. a WiFi enabled device), to connect with other devices. Similar to the BlackBerry Messaging (“BBM”) service, WhatsApp allows users to send text messages, multimedia (pictures, videos, audio messages, etc.), location information, and share contacts with one another free of traditional SMS or multimedia messaging service (“MMS”) service rates. Unlike the BBM service, however, which only allows BlackBerry users to connect with other BlackBerry users, WhatsApp connects a wide range of devices produced by multiple telecommunications companies, so long as each device has installed the WhatsApp Messenger application. In other words, an Apple iPhone and a BlackBerry device can communicate and share an infinite amount of data with one another in an SMS format, but free of SMS service rates. This allows for video, audio, and other content to be dispersed very widely and globally. WhatsApp also allows the users to establish private groups similar to an email thread or messaging board;

- d. WhatsApp maintains electronic records pertaining to individuals and companies for which they maintain subscriber accounts. These records may include account access information (IP addresses), account holder name, account holder email address, message strings, images, video files, attached files, voice messages, chats, chat groups, service start date, group chat information, and address book;
- e. Subscribers to WhatsApp may access their accounts on servers maintained or owned by WhatsApp from the “smartphones” containing the telephone number from which they subscribed to the account and from anywhere in the world; and
- f. Text messages, images, pictures, videos, and audio messages stored in the subscriber’s WhatsApp account are stored on WhatsApp’s servers, up to thirty (30) days, until delivered to the intended recipients and then are deleted from the WhatsApp servers.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2713 by using the warrant to require WhatsApp to disclose to the government copies of the records and other information (including the content of communications if available) described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

59. This application seeks a warrant to search all responsive records and information under the control of WhatsApp, a provider subject to the jurisdiction of this court, regardless of where WhatsApp has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within WhatsApp’s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

CONCLUSION

60. Based on the information described above, I request that the Court issue the proposed search warrant for the accounts listed in Attachment A. Because the warrant will be served on WhatsApp, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

61. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following phone numbers and for the following periods, that are stored at premises controlled by WhatsApp, a company that accepts service of legal process at 1601 Willow Road in Menlo Park, California.

1. **(202) 921-0123** (from January 1, 2016 to present)
2. **(202) 753-9708** (from January 1, 2016 to present)
3. **+91-7054210000** (from January 1, 2016 to present)
4. **+91-8765919198** (from January 1, 2016 to present)
5. **+91-9044971271** (from January 1, 2016 to present)
6. **+54-911 36594384** (from January 1, 2016 to present)
7. **+90-5368406561** (from January 1, 2016 to present)
8. **+91-7304096699** (from June 1, 2018 to present)
9. **+91-9356460394** (from June 1, 2018 to present)
10. **+34-691962857** (from June 1, 2018 to present)
11. **+44-7490620584** (from August 1, 2019 to present)

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by WhatsApp (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each of the accounts or identifiers listed in Attachment A:

- a. All stored electronic communications (including drafts, sent items, deleted items, stored backup copies, and attachments) and other stored content information contained in or on behalf of the accounts.
- b. All histories, profiles, contact lists, email addresses, attachments, screen names, name, age, telephone number, physical address, or user IDs, associated with the accounts;
- c. Logs of all access to the accounts, including but not limited to all electronic communications sent to or from the account, including dates, times of access, and the Internet Protocol addresses (IP addresses) from which the account was accessed, for the accounts;
- d. All transactional information concerning activity associated with the accounts, including log files, dates, times, methods of connecting, or locations, for the accounts;
- e. All business records and subscriber information, in any form kept, concerning the accounts, including applications, account creation date and time, all full names, screen names, and account names associated with the subscribers, profile photos, contact lists, group chats, methods of payment, telephone numbers, addresses, and detailed billing records, for the accounts; and
- f. All records indicating the services available to subscribers of the account.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 841(a)(1), 841(h), and 843(c)(2)(A), including but not limited to:

- a. The sale and distribution of controlled substances;
- b. The exchange or laundering of funds related to the sale and distribution of controlled substances;
- c. Evidence indicating how and when the WhatsApp account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the WhatsApp account owner;
- d. Evidence indicating the WhatsApp account owner's state of mind as it relates to the crimes under investigation;
- e. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s)
- f. Other accounts used by the persons using the account;
- g. The devices used to access the account;
- h. The identity of the person(s) who communicated with the account about matters relating to the sale and distribution of controlled substances, including records that help reveal their whereabouts;
- i. Financial information, credit card numbers, social security numbers, and other personal identifiable information stored on/in the WhatsApp account; and
- j. Communications and files that contain IP addresses and username and passwords.